Algebra 2 - Compitino 3/5/2011

Nome e Cognome: Matricola:

Rispondere su questo foglio usando gli appositi spazi e giustificando brevemente ma esaurientemente tutte le risposte.

1 Sia G un gruppo con 8 elementi non ciclico.

1.1 Dimostrare che se $g \neq 1$ allora $o(g) \in \{2, 4\}$.

Il periodo di g divide $|G|$ (Lagrange). Quindi $o(g) \in \{1, 2, 4, 8\}$.
Ma $o(g) = 1 \to g = 1$, escluso e $o(g) = 8 \to G$ ciclico, escluso. Quindi la tesi.

1.2 Sia $o(g) = 2$ per ogni $g \in G$. Dimostrare che $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. (Aiuto: siano $a, b \neq 1$, $a \neq b$ in G e $c \notin < a, b >$. Considerare i sottogruppi $< a, b >$ e $< c >$...)

$o(g) = 2$ $\forall g \neq 1 \Rightarrow G$ abeliano. Infatti $(xy)^2 = 1 \to xy = y^{-1}x^{-1} = yx$ $\forall x, y \in G$.
Uso l'aiuto: $<a,b> = \{1, a, b, ab\}$ e $<c> = \{1, c\}$ sono normali con intersezione $= \{1\}$; quindi
$G = <a,b><c>$, da cui $G = <a,b> \times <c> \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

1.3 Supponiamo che esista un elemento $g \in G$ tale che $o(g) = 4$ e sia $h \notin < g >$. Dimostrare che $G =< g > \cup h < g >$ (unione disgiunta).

$|<g>| = 4 \to [G : <g>] = 2 \to <g>$ ha solo due laterali distinti:
$<g>$ e $h<g>$ con $h \in G \setminus <g>$, da cui la tesi.

1.4 Assumendo 1.3, dimostrare che se $gh = hg$ allora $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. $G = \{1, g, g^2, g^3, h, hg, hg^2, hg^3\}$

$gh = hg \Rightarrow G$ abeliano. 1° caso: $o(h) = 2 \Rightarrow G = <g> \times <h>$ (come in 1.2).
2° caso: $o(h) = 4$, allora $h^2 \notin h<g>$ perché $h \notin <g>$ e siccome $o(h^2) = 2$, si ha $h^2 = g^2$.
Da cui $(hg)^2 = h^2 g^2 = g^4 = 1 \to o(hg) = 2 \to G = <g> \times <hg>$. In ogni caso si ha la tesi.

1.5 Assumendo 1.3, dimostrare che $h^{-1}gh \in < g >$.

$<g> \lhd G$ perché ha indice 2 $\longrightarrow x^{-1}gx \in <g>$ $\forall x \in G$.
In particolare ciò vale per $x = h$.

1.6 Assumendo 1.3 e $gh \neq hg$, dimostrare che $h^{-1}gh = g^{-1}$.

$h^{-1}gh = 1 \to g = 1$ no! $h^{-1}gh = g \to gh = hg$ no!
$h^{-1}gh = g^2$ che ha periodo 2 $\to (h^{-1}gh)^2 = 1 \to h^{-1}g^2h = 1 \to g^2 = 1$ no!
Rimane solo la possibilità $h^{-1}gh = g^3 = g^{-1}$.

2 Sia $\mathbb{Z}_5$ il gruppo additivo delle classi di resti modulo 5. Si dica se le seguenti leggi definiscono un'applicazione di $\mathbb{Z}_5$ in $\mathbb{Z}_{10}$. In caso affermativo, dire se sono omomorfismi di gruppi, e se sono iniettivi o no.

2.1 $f_1 : [x]_5 \mapsto [x]_{10}$. non è ben definita:

$[1]_5 = [6]_5$, però $f[1]_5 = [1]_{10}$ e $f[6]_5 = [6]_{10}$ e $[1]_{10} \neq [6]_{10}$

Quindi non può essere un omomorfismo.

2.2 $f_1 : [x]_5 \mapsto [2x]_{10}$. è ben definita:

$[x]_5 = [y]_5 \to x - y = 5k \to 2x - 2y = 10k \to [2x]_{10} = [2y]_{10}$.
Rispetta la somma: $f([x]_5 + [z]_5) = f[x+z]_5 = [2x+2z]_{10} = [2x]_{10} + [2z]_{10} \longrightarrow$
$\to$ è un omomorfismo. $\operatorname{Ker} f = \{ [x]_5 \mid 2x = 10k, k \in \mathbb{Z} \} \longrightarrow$
$\to \operatorname{Ker} f = \{ [x]_5 \mid x = 5k, k \in \mathbb{Z} \} = \{[0]_5\}$ e f è iniettivo.

3 Sia $G = \mathbb{Z}_{12}$, il gruppo delle classi dei resti modulo 12 rispetto alla somma.

3.1 Elencare i sottogruppi di G indicando per ciascuno un generatore.

$G_1 = <[0]>$, $G_2 = <[1]> = \mathbb{Z}_{12}$ sottogruppi banali
$G_3 = <[2]>$ di ordine 6 , $G_4 = <[3]>$ di ordine 4 , $G_5 = <[4]>$ di ordine 3
e $G_6 = <[6]>$ di ordine 2.

3.2 I sottogruppi sono normali?

Sì, perché G è abeliano.

3.3 Elencare tutti gli automorfismi di G.

$Aut(\mathbb{Z}_{12}) \simeq \{U_{12}, \cdot\}$ ← gruppo moltiplicativo degli invertibili di $\mathbb{Z}_{12}$.
I suoi elementi sono $f[x]_{12} = [kx]_{12}$ con $(k, 12) = 1$, cioè $k = 1, 5, 7, 11$.

4 Siano $A =< \alpha >$ e $B =< \beta, \gamma >$ dove α, β, γ sono le permutazioni:

$$\alpha = (1234) \qquad \beta = (567) \qquad \gamma = (56)$$

4.1 Si determinino i periodi di α, β e γ.

Il periodo di un ciclo è uguale alla sua lunghezza:
$o(\alpha) = 4$, $o(\beta) = 3$, $o(\gamma) = 2$.

4.2 Si scrivano tutte le potenze distinte di α, β e γ.

α, $\alpha^2 = (13)(24)$, $\alpha^3 = (1432)$, $\alpha^4 = id$.
β , $\beta^2 = (576)$, $\beta^3 = id$. γ, $\gamma^2 = id$.

4.3 Qual è l'ordine di B? B è ciclico? A quale gruppo è isomorfo?

$B = <\beta, \gamma> \to B \supset <\beta>$ e $B \supset <\gamma> \to$ per Lagrange $3 \mid |B|$ e $2 \mid |B| \to$
$\to |B| = 6k$. Ma $B \subseteq$ gruppo simmetrico su 3 lettere $\{5, 6, 7\} \to |B| \leq 6 \to$
$\to |B| = 6$. Quindi $B = Sim\{5, 6, 7\}$ che non è ciclico ed è isomorfo a S_3.

4.4 Si provi che $< \beta >$ è un sottogruppo normale di B.

$|<\beta>| = 3 \to [B : <\beta>] = 2 \to <\beta> \trianglelefteq B$.

4.5 Si mostri che il prodotto AB è un gruppo. Di che ordine?

I gruppi $A = <\alpha>$ e $B = <\beta, \gamma>$ sono permutabili perché gli elementi di A e quelli di B operano su numeri distinti. Ne segue che $AB = <A, B>$ e AB è un gruppo.
Poi $A \cap B = \{id\}$ e $|AB| = \dfrac{|A| \cdot |B|}{1} = 4 \cdot 6 = 24$.

5 Sia $G = GL(2, \mathbb{Z}_3)$, il gruppo delle matrici quadrate non singolari di ordine 2 sul campo $\mathbb{Z}_3$ delle classi dei resti modulo 3 rispetto all'usuale prodotto righe per colonne e si consideri il sottoinsieme

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} | a, b, c \in \mathbb{Z}_3 \quad ac \neq 0 \right\}.$$

5.1 Si provi che H è un sottogruppo di G.

H non è vuoto: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$. Inoltre $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} = \begin{pmatrix} a\alpha & * \\ 0 & c\gamma \end{pmatrix}$ con $a\alpha c\gamma \neq 0$ perché per ipotesi $ac \neq 0$ e $\alpha\gamma \neq 0$. $\longrightarrow$ H è chiuso rispetto al prodotto. Poiché H è un insieme finito basta questo per provare la tesi.

5.2 H è normale in G? Qual è il suo ordine?

H non è normale in G. Controesempio: $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} =$
$= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix} \notin H.$

$|H| = 12$ perché ho 3 scelte per b, 2 per a e 2 per c.

5.3 Costruire $Z(H)$, il centro di H.

$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \quad \forall a, b, c \in \mathbb{Z}_3$ con $ac \neq 0$.

$\begin{pmatrix} xa & xb+yc \\ 0 & zc \end{pmatrix} = \begin{pmatrix} ax & ay+bz \\ 0 & cz \end{pmatrix} \rightarrow xb + yc = ay + bz \quad \forall a,b,c;\ ac \neq 0$

In particolare se $b=0$, $a=1$ e $c=2 \rightarrow y=0$, da cui $b(x-z)=0 \ \forall b \rightarrow x=z$

$$Z(H) = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \ \begin{matrix} x \in \mathbb{Z}_3 \\ x \neq 0 \end{matrix} \right\}$$

5.4 Provare che $H/Z(H)$ è isomorfo ad S_3.

$\left|\frac{H}{Z(H)}\right| = 6$ perché $|Z(H)| = 2$, quindi ci sono solo due possibilità

1) $\frac{H}{Z(H)}$ ciclico, ma ciò implica H abeliano: falso!

2) $\frac{H}{Z(H)} \simeq S_3$.

5.5 Determinare il gruppo degli automorfismi interni di H.

$$\mathrm{Int}(H) \simeq \frac{H}{Z(H)} \simeq S_3.$$

6 Sia $G = (\mathbb{Z}_{37}^*, \cdot)$ il gruppo moltiplicativo degli elementi invertibili nel campo $\mathbb{Z}_{37}$.

6.1 Si provi che il periodo di $x = 3$ è 18. (congruenze modulo 37)

Poiché $|G| = 36$ i periodi possibili sono $1, 2, 3, 4, 6, 9, 12, 18, 36$.
$o(x) \neq 1$. $3^2 = 9$, $3^3 = 27$, $3^4 = 81 \equiv 7 \to o(x) \neq 2, 3, 4$.
$3^6 \equiv 63 \equiv 26 \to o(x) \neq 6$
$3^9 \equiv 26 \cdot 27 \equiv 36 \equiv -1$, quindi $o(x) > 9$ e $3^{18} = 1$ e poiché $12 \nmid 18$ si ha che $o(x) = 18$.

6.2 Si calcoli il periodo di $y = 6$.

6, $6^2 = 36 \equiv -1 \to 6^4 \equiv 1 \to o(y) = 4$

6.3 Siano x e y come sopra, si costruisca un generatore di G.

$|G| = 36 = 4 \cdot 9$ con G abeliano e $MCD(4, 9) = 1$.
Poiché $o(x) = 18 \to o(x^2) = 9$. Ne segue che
$o(x^2 y) = 9 \cdot 4 = 36$
Un generatore è $x^2 y = [54]_{37} = [17]_{37}$.

OSSERVAZIONI

1) Negli es. 1.2 e 1.4 G è abeliano. La risposta può essere immediata utilizzando la struttura dei gruppi abeliani finiti. Infatti esistono solo 3 gruppi abeliani di ordine 8 a due a due non isomorfi:

$$G_1 \simeq \mathbb{Z}_8 \,, \quad G_2 \simeq \mathbb{Z}_4 \times \mathbb{Z}_2 \,, \quad G_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 .$$

G non è ciclico per ipotesi $\longrightarrow G \neq G_1$.

Nel punto 1.2 G non ha elementi di periodo 4 $\longrightarrow G \simeq G_3$.

Nel punto 1.4 G ha un elemento di periodo 4 $\longrightarrow G \simeq G_2$.

2) Nell'es. 2 si può applicare il criterio:

$f : \mathbb{Z}_n \to \mathbb{Z}_m$ dato da $f[x]_n = [kx]_m$ è un omomorfismo ben definito se e solo se $m \mid k \cdot n$.

Ed è iniettivo se e solo se $m = n \cdot \mathrm{MCD}(k, m)$.

3) Nell'es. 4.3 <u>non</u> è corretta l'implicazione

$$o(\beta) = 3 \,, \quad o(\gamma) = 2 \,, \quad (3,2) = 1 \implies |\langle \beta, \gamma \rangle| = 2 \cdot 3 = 6 .$$

Controesempio:

$$\beta = (5\,6\,7) \,, \quad \gamma = (5\,8) \longrightarrow |\langle \beta, \gamma \rangle| \geq 12$$

perché $\langle \beta, \gamma \rangle$ contiene un elemento di periodo 4:

$$(5\,6\,7)(5\,8) = (5\,6\,7\,8) .$$